Analysis of COVID-19 Tracking Tool in India: Case Study of Aarogya Setu Mobile Application

RAJAN GUPTA, Deen Dayal Upadhyaya College, University of Delhi, India
MANAN BEDI, PRASHI GOYAL, SRISHTI WADHERA, and VAISHNAVI VERMA,
Shaheed Sukhdev College of Business Studies, University of Delhi, India

COVID-19 tracking tools or contact-tracing apps are getting developed at a rapid pace by different governments in their respective countries. This study explores one such tool called *Aarogya Setu*, developed by the Government of India. It is a mobile application developed under the Health Ministry, as a part of the E-Governance initiative, to track and sensitize the citizens of India in a joint battle against COVID-19 spread. The study aims to understand various useful features of this tool and to present different concepts of data science applied within the application along with its importance in managing the ongoing pandemic. The App uses Bluetooth and GPS technologies to alert a user when they are nearby a COVID-19 infected person. The application uses various Data Science concepts such as Classification, Association Rule Mining, and Clustering to analyze COVID-19 spread in India. The study also shows potential upgradations in the application, which includes usage of Artificial Intelligence and Computer Vision to detect COVID-19 patients. The study would be useful for mobile technology professionals, data science professionals, medical practitioners, health-related frontline workers, public administrators, and government officials.

CCS Concepts: • **Social and professional topics** → **Governmental surveillance**; • **Applied computing** → **E-government**;

Additional Key Words and Phrases: E-Governance, India, coronavirus, contact-tracing, tracking tool, Bluetooth, GPS, COVID-19 reporting tool, Aarogya Setu

ACM Reference format:

Rajan Gupta, Manan Bedi, Prashi Goyal, Srishti Wadhera, and Vaishnavi Verma. 2020. Analysis of COVID-19 Tracking Tool in India: Case Study of *Aarogya Setu* Mobile Application. *Digit. Gov.: Res. Pract.* 1, 4, Article 28 (August 2020), 8 pages.
<https://doi.org/10.1145/3416088>

1 INTRODUCTION

The contagious coronavirus, or more technically known as COVID-19, has spread all over the world and is listed as a pandemic by the World Health Organization [1]. It started surfacing in China in November 2019 and has been on the rise in all major parts of the world. On 27th July, 2020, more than 16.52M cases of COVID-19 were reported in about 187 countries and territories [2]. On 30th January, 2020, the first case of coronavirus pandemic in India

Authors' addresses: Dr. R. Gupta, Department of Computer Science, 4th Floor, Deen Dayal Upadhyaya College, University of Delhi, Azad Hind Fauj Marg, Sector-3, Dwarka, Delhi-110078, India; email: guptarajan2000@gmail.com; M. Bedi, P. Goyal, S. Wadhera, and V. Verma, Shaheed Sukhdev College of Business Studies, Dr. K.N. Katju Marg, Rohini Sector 16, PSP Area IV, New Delhi, Delhi-110089, India; emails: {mananbedilps, goyalprashi, srishtiwadhera, vaishuverma13616}@gmail.com.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2020 Association for Computing Machinery.

2639-0175/2020/08-ART28 \$15.00

<https://doi.org/10.1145/3416088>

Digital Government: Research and Practice, Vol. 1, No. 4, Article 28. Publication date: August 2020.

was reported, and the number of cases in India has now reached more than 1.48M [3]. Most people infected from COVID-19 experience mild to moderate respiratory illness. If a person is tested positive for coronavirus, every individual who has come in contact with the infected individual is advised to go for self-quarantine for two weeks, so that the infection chain can be broken and the disease does not spread further. At present, there is no specific treatment or vaccine available for COVID-19. Many countries are trying to develop contact-tracing techniques through which they can trace the person suspected of the infection. For example, in South Korea, the government is maintaining a database of known patients along with their details such as their age, gender, occupation, and so on. [4] In Israel, the government has been allowed to track the mobile-phone data of people suspected with the infection [5]. Singapore developed a mobile-based application, TraceTogether, which tracks via Bluetooth whenever two application users are nearby [6]. If a person's report is diagnosed with COVID-19, a human contact tracer can then determine follow-up actions.

A similar kind of mobile tracing application has been developed in India, namely, *Aarogya Setu* [7, 8]. The App is designed in such a way that it informs the user whenever they come in contact with an infected person through Bluetooth and GPS location services. The data acquired from the application is not disclosed publicly and is only used by the government for tracing, tracking, and management of COVID-19. There are necessary steps that need to be followed by the users to use the *Aarogya Setu* application by logging into the App using a one-time password and filling out basic demographic details of the users to suggest whether the user is in safe vicinity or not. Given the foreign travel history, if it exists for the user, it is matched with those who have been tested positive for COVID-19 with the help of the Indian Council of Medical Research (ICMR) database. This article presents an analysis of the *Aarogya Setu* App.

2 ABOUT AAROGYA SETU APP

The *Aarogya Setu* App is a COVID-19 (coronavirus) mobile tracking application developed by the National Informatics Centre (NIC), which is under the Ministry of Electronics and Information Technology, Government of India. The *Aarogya Setu* application can be downloaded from the Google Play Store [9] as well as from the App Store [10] for iOS devices. Currently, the App is available in 12 Indian languages, which are English, Tamil, Hindi, Telugu, Kannada, Malayalam, Punjabi, Bengali, Oriya, Gujarati, Marathi, and Assamese. It is expected that it will be available in more Indian languages soon.

The application has been designed in such a way that it informs the users through notification if they cross paths with a COVID-positive person. The tracking is accomplished with the help of Bluetooth technology and location-generated social graphs or GPS, which shows the user's interaction with anyone who has been tested coronavirus positive and notifies them. It detects and tracks the user's movement with the help of GPS and Bluetooth sensors. It will also discover other nearby smartphones that also have the application installed and then sends out a notification if they come in contact with infected people by using its database and algorithms. The App also provides essential instructions on how to self-isolate and what should be done in case anyone develops symptoms. The App recommends to keep the Bluetooth and the Location services on at all times. To use the application, one must register with a mobile number by verifying through an OTP.

A form in the App asks for personal details from the user, such as name, age, occupation, foreign travel history in the last 30 days, and other profiling information. There is also a "Self-Assessment Test" feature on the *Aarogya Setu* Application in which some questions related to the health and symptoms of the user are asked, and based on the answers, the application shows the risk level for the user in different color codes. There is no risk if it indicates green color code and the text shows "You are safe." There is low risk if it shows yellow color code and the version shows "You are at moderate risk." There are high chances of risk if it shows an orange color code; then the user must contact the help-line number given in the App. The application also suggests specific actions that can be taken to stop the spread of coronavirus, such as social distancing, taking care of hygiene, and staying at home as precautions. As mentioned in the application's privacy policy, the data that is acquired through the form is shared only with the Government of India and will not be disclosed to any third party. The

data will provide support to the government for taking appropriate steps and initiate the isolation procedure, if necessary. The name and number of the user will not be disclosed publicly.

Aarogya Setu has four sections: Your Status, Self-Assess, COVID-19 Updates, and E-Pass. The “Your Status” section tells the user his/her risk of getting COVID-19. The “Self-Assess” section tells the user about the risk of getting infected. The COVID-19 Update section gives updates on the local and national COVID-19 cases, while E-Pass helps in getting a movement pass in case of emergencies. So that other computer programs like web services and mobile applications can make use of the data available and other features of *Aarogya Setu*, the App has been built on a platform that can provide an Application Programming Interface (API) to support different applications.

3 PROMINENT FEATURES

3.1 Tracking Features

The application uses the secured database of the Government of India, wherein it stores the data identified with known cases and suspected cases. To prevent the application and its associated data from malicious hacking attempts, the government has not made the database or any other information related application as open-source. Not much is known about the technicalities of the App due to its secured nature. The only details that are known about the App come from press reports, front-end analysis, and terms and conditions of the application. The application uses both Bluetooth and GPS-generated data for contact-tracing to alert users if they come in contact with a person suffering from COVID-19 or with someone who is at high risk of getting COVID-19. The Bluetooth and GPS of the user’s device must always be turned on for the App to function correctly. Bluetooth access is a significant key for the application to build up information on proximity between two individuals. At the point when two cell phones, which have the App installed, come in one another’s Bluetooth range, the application collects data. If anyone of the users is tested positive, the App cautions the other user, and this helps the government in keeping track of potential COVID-19 cases. Along with these cautions, the application also has guidelines for any symptoms of the virus found in their vicinity. Besides Bluetooth and location data, the App collects the demographic data from the users, such as their gender, phone number, age, full name, and foreign travel history. It also asks the user if they are engaged in providing essential services and if they would be willing to help in times of need. The government can, subsequently, download this data to trace potential cases and discover volunteers who are eager to assist in the time of crisis.

More evidence on the effectiveness of proximity tracing tools such as Bluetooth and GPS has been referred, as proximity is not solely responsible for contagion; the risk may be dependent on other independent factors such as being in an enclosed or open space. A limited user base, attributed to the low rate of adoption, can significantly reduce the effectiveness of the App [16]. Bluetooth-based apps rely on the Neighbor Discovery protocol provided by smartphones. Hence, the accuracy of discovery and emission of signals varies significantly in different smartphones. The protocol determines the level of energy consumption (i.e., how long the battery will last), the reliability of operation when multiple phones are close to the cell’s receptor, and how quickly two phones can discover each other when they come nearby [17].

Proximity-based apps can generate a lot of false negatives and false positives. Distance is estimated based on the attenuation of the wireless signal in free space. However, the signal can also be largely attenuated by human bodies. If two individuals are standing with their back towards each other, the signal can become weak, and the distance between them can be misinterpreted, resulting in a false negative. The accuracy of the App depends on the positioning of smartphones concerning each other (e.g., whether the phone is in one’s bag or hands). For example, a thin wall across two apartments may not attenuate the signal enough, and it could result in a proximity event, even when it is not. False positives can lead to the isolation of unaffected people, and false negatives hamper the main objective of the application.

Bluetooth-based systems are usually more accurate than GPS-based methods. Bluetooth-based tracking apps have a lower false-positive rate, consume less power, and have a better standard of adoption than GPS-based tracking apps. Besides the privacy concerns regarding GPS tracking, GPS data is inaccurate and unavailable

inside buildings [17, 18]. Bluetooth is used by 57% of contact-tracing apps, whereas 43% of the apps use GPS [19]. There is a significant trade-off between information and privacy in GPS-based applications. While privacy is a big concern, applications that use only Bluetooth cannot provide information about the geographical movement of people, which is crucial for contact-tracing.

Contact-tracing applications that use both Bluetooth and GPS are much more useful than applications that use only Bluetooth. Location data coupled with proximity history can help health authorities in identifying exposure trails with higher accuracy. Hence, the technology on which *Aarogya Setu* App is working seems to be mostly fine.

3.2 Comparative Analysis with Other Apps

A detailed analysis of other applications similar to *Aarogya Setu* can help us delineate or to understand better the working of the application and how it analyzes its data. *TraceTogether* is an application that supports Singapore's efforts in mitigating the effects of the ongoing pandemic. Like *Aarogya Setu*, *TraceTogether* uses Bluetooth signals to determine when the user's phone is near another phone that also has the application installed. Both phones exchange anonymized IDs, which are then stored in an encrypted form, only on the user phone through cryptographic techniques. A plus point of the application is that the anonymized IDs expire within 15 minutes of generation so that hackers are not able to manipulate the data. *Private Kit: Safe Paths* [11] is another application that has been developed by the Massachusetts Institute of Technology. This application also lets the user know whenever they come in contact with an individual who is COVID positive. The App seeks to simplify the contact-tracing procedure. Contact-tracing is an essential tool for diminishing the spread of infectious diseases. This application uses GPS-based arrangement. In any case, since GPS information is more challenging to anonymize, the application developers are investigating specialized technical solutions along the lines of more grounded encryption. *Private Kit: Safe Paths* gathers users' location information by keeping a time-stamped log within every five minutes. Altogether, 28 days of data can be put away in the application in less than 100 kilobytes of storage space (which is less than the storage space taken by a single photo). The information of the user never leaves the phone and is encoded with the goal that other users cannot recognize the user. On the off chance that a user ends up testing positive for COVID-19, the user can send location information to public health researchers with the help of a QR code. In this way, it facilitates contact-tracing.

Comparative analysis shows that *Aarogya Setu* differs in some aspects compared to its counterparts, i.e., *Private Kit* and *TraceTogether*. Concerns regarding data privacy have been handled differently in *Aarogya Setu* App as per the global claims, which suggests that contact-tracing applications can be highly invasive. It leads to the belief that the government of the respective apps might be monitoring all user data collected by the application, and that has to be done; otherwise, the contact-tracing activity may not be fruitful for any such App. Unlike *TraceTogether* and *Private Kit: Safe Paths*, contact history data in *Aarogya Setu* App may not be private to the individuals using the application. The government may be utilizing the data collected from GPS to identify major hotspots of infected people in the country and, subsequently, barricading those areas to prevent further spread of the disease. Based on the comparisons, it can be concluded that data policy in each country will impact the designing of such types of apps [12, 13].

Comparing some other apps developed by different nations for COVID tracing on various parameters is as follows.

- **Data Destruction:** The data that the App collects should be automatically deleted in a reasonable amount of time (maximum 30 days), or the App allows users to delete their own data manually. Some countries that automatically destroy the data are Australia, Canada, India, Israel, Italy, and Japan. Countries that do not destroy the data are Belgium, China, France, Germany, and UK.
- **Transparency:** It can take the form of clear, publicly available policies and design, an open-source code base. Countries whose apps are transparent are Austria, Canada, India, Israel, Poland, and Singapore. Apps that are not transparent belong to Australia, China, France, Malaysia, and Norway.

- **Limitations on Data Collection:** Data may sometimes be used for purposes other than public health such as law enforcement—and that may last longer than COVID-19. Countries that are limited in Data Collection: Australia, Bulgaria, Denmark, Israel, and Switzerland. Countries that have not limited Data Usage: Algeria, Belgium, China, Finland, and Hungary. For India, it is not clear.
- **Underlying Technology:** Some apps identify a person's contacts by tracking the phone's movements like GPS. Some systems use "proximity tracking," in which phones swap encrypted tokens with any other nearby phones over Bluetooth. Many apps rely on the standard API that Apple and Google are developing. Some use DP-3T, which is a decentralized privacy-preserving proximity tracing. Countries that are using only Bluetooth technology for locations include Australia, Czechia, and France. Austria and Belgium uses Bluetooth along with the common API from Google or Apple. India used both Bluetooth and GPS [24].

3.3 Data Science Techniques

The primary goal in contact-tracing is to find major "hotspots" of COVID-19 patients and impose appropriate measures on these hotspots to curb further spread of the infection. With the help of the longitude and latitude coordinates of COVID-19 patients and at-risk people, clusters can be created with the help of some Artificial Intelligence and Machine Learning Techniques [14]. These clusters can then be considered as hotspots. To find groups, unsupervised machine learning models like K-means clustering can be used to make clusters of infected people. There is a probability that the density-based function HDBSCAN (based on the DBScan algorithm) may have been used in the development of the application, or can be used in similar forms. Also, the self-assessment test, based on the ICMR guidelines, evaluates the likelihood of COVID-19 infection based on the user's self-reported symptoms and other relevant information such as recent travel, age, and gender. A classification model such as decision tree or random forest could have been used to classify the users into zones such as green (safe), yellow (moderate risk), orange (high risk), and red (confirmed patients). The users have to answer the above questions in the self-assessment test. This evaluation takes place on the application, and the results are communicated to the users immediately in terms of green, yellow, or orange colors, indicating progressively higher probabilities of infection. Based on the answers given by the users, the App performs classification.

With further research, it could be inferred that the application may be using a protocol called iBeacon [15] for the collection of Bluetooth-proximity data. It is a protocol that was developed by Apple. Various vendors (including Android) have made iBeacon-compatible hardware transmitters (called beacons—a class of Bluetooth Low Energy Devices). This device consistently broadcasts a Bluetooth 4.0 signal (BLE) and its unique identifier to nearby portable electronic devices; whereas most Bluetooth devices require a process called "pairing" for data transfer, in which the owner of the device has to confirm the exchange on both devices for the action to proceed. An iBeacon's communication is one-way, meaning that an iBeacon could transfer information to a receiver device (such as a mobile phone, a laptop, etc.) without the need for pairing, making the process significantly more straightforward. The technology enables smartphones, tablets, and other devices to perform actions when in proximity to an iBeacon. The universally unique identifier is then picked up by the compatible application, i.e., *Aarogya Setu*. The ID and several bytes sent with it can be used to determine the device's physical location, track users, or trigger a location-based action on the device such as a push notification. In the application, users are notified whenever they're too close to a person infected from coronavirus or someone who is at high risk. Bluetooth proximity history data (identification tags, signal strength, etc.) will eventually be published to a secure database where information can be retrieved by the Government of India or the organization that developed the application. After extracting that data, the government may perform data analysis on it.

3.4 Privacy Concerns & Features

The *Aarogya Setu* app collects certain personal information about the user, which includes name, phone number, age, sex, profession, countries visited in the past 30 days, current medical condition of the user, and stores it in the

cloud. The user's location details are also accessed at the time of registration. Moreover, the App continuously tracks the user's location through GPS/Bluetooth and maintains a record of the movement of the user. This may lead to severe implications for data protection. People having access to such data may deduce the user's home and work address, socioeconomic status, identity (religion or caste), and much more. The inclusion of the sensitive nature of data and the mandatory prescription for using the App raises concerns about privacy violations. Invasion into people's privacy vis-a-vis health records can have terrible effects on a person's standing in society and can lead to discriminatory outcomes.

India witnessed indiscriminate sharing of the lists of persons suffering from coronavirus through digital means. And such privacy risk can lead to acute harm, as the information may be misused. The state-level authorities are disclosing the user details such as name, home, and address of those who are put under quarantine, which has led to the illegal sharing of data. Moreover, it opposes the right to privacy judgment passed by the Supreme Court of India. The App does not fulfill the proportionality test under the Right to Privacy that states *that the action must be sanctioned by law, must have a legitimate aim, the extent of such interference must be proportionate to the need for such interference, and there must be procedural guarantees against abuse of such interference*. The absence of any legislation governing this App leads to the possibility of its misuse, according to the fulfillment of the proportionality test. India lacks a comprehensive personal data protection framework, which causes a violation of rules. The extensive amount of personal information that the App secures is against the norm of data minimization, purpose limitation, transparency, and accountability as well. The absence of any governing legislation, the terms of service, and privacy policy account for the data security issue [25].

However, the App is incorporated with features to protect the personal privacy of the users. It generates a unique device ID number. When a user comes in contact with someone, this ID is sent to his or her device, not the user's name and phone number. The location information on the App gets deleted on a 30-day rolling cycle. The *Aarogya Setu* app has been made an open-source now, which would allow the developers to understand how it works and how data is processed through it. This signifies the government's commitment to transparency [26]. A few improvements have been made in the revised version of the App. The information is no longer hashed to a unique ID, but it still uses a device ID. The privacy policy no longer claims that personal data is mapped in this way. Now, only on reporting COVID-19 positive status, or on requesting a test, the information will be uploaded to the server, which includes the user's location data that is collected every 15 minutes and stored on the device itself, and details of all DiD exchanges with people a user got near. Except for the DiD, the personal information of other users will NOT be uploaded to the server. This information will be deleted after 60 days if a person tests positive and gets cured, or after 45 days if a person tests negative [27].

3.5 Compatibility with Apple & Android Playstore

Aarogya Setu app is available for both iOS and Android users. The application currently supports Android 5.0 and above versions and iOS 10.3 and above versions. It relies on certain vital features and functionalities that are not supported in older versions of Android/iOS. A version of the application for KaiOS will be made available soon [20].

Google and Apple have collaborated to create a two-stage Exposure Notification solution that utilizes Bluetooth technology on mobiles to assist with contact-tracing efforts. In the primary stage, both companies released APIs that permitted contact-tracing applications of public health authorities to work across Android and iOS devices while maintaining user privacy. In the subsequent stage, which will be accessible in the coming months, this capability will be introduced at the operating-system level to help ensure broad adoption. After a consent-based operating system update, the system will send out and listen for the Bluetooth beacons as in the primary stage, but without requiring an application to be installed [23].

The Bluetooth-based methodologies that do not utilize the Apple–Google framework will be constrained by limitations in Bluetooth scanning on iOS-based smartphones. Applications running on iOS can scan for nearby

Bluetooth devices only if the application is visible on the screen (foreground) or when the application is not visible (background) if the target device is explicitly specified. Given that target devices are commonly not known by the scanning device before detection, this prevents iOS-based devices with background contact-tracing apps from detecting one another [21].

The API has been embraced by several countries such as Australia, Austria, Brazil, Canada, Croatia, Denmark, Germany, Ghana, Ireland, Italy, Japan, Kenya, Latvia, Philippines, Poland, Saudi Arabia, Switzerland, the UK, and Uruguay, with many of them building up their contact-tracing applications based on the Exposure Notification protocols [22]. However, the API is not compatible with the *Aarogya Setu* application. *Aarogya Setu* has not connected to the Apple-Google API. The difference is that the Exposure Notification solution does not collect the location details of its users. However, *Aarogya Setu* does collect the location details of its users. This is because the application has to undergo a few tweaks in terms of the underlying technology and privacy to be compatible with the API.

Hence, there are a couple of changes and requirements that *Aarogya Setu* needs to satisfy so that it can be compatible with Google's API, but they are not required on an urgent basis.

4 DISCUSSION & CONCLUSION

Aarogya Setu Application slightly differs from "Privacy-focused Global Standards" restricted only to Bluetooth-based technology using GPS Trails. It can easily match devices by not revealing the exact location of the cell-phone. GPS trails are not at all reliable in indoor settings or mass transit situations. Such devices are prone to hacking. In some cases, some information could be uploaded to a cloud server, which can be extracted and misused. The data collected by the application is stored both on the device and the central server. The encrypted user data on its servers could last beyond the purpose of tracing coronavirus. It can also be concluded that it is a promising application that can help people to be safe from coronavirus. Apart from some improvements with better Deep Learning techniques employed and fixing data privacy issues in a more secure manner, the application has useful features and impressive architecture. It is evident from the beautiful user interface (UI) that user-interactivity was properly kept in mind during the development of the application.

The application, overall, helps the government in keeping track of people who have been tested positive for the virus. It is also an excellent way to alert people about the number of infected cases in their area that have been identified as coronavirus-positive or if they accidentally came in contact with a person suffering from COVID-19. The application requires being in running mode at all times to continue tracing individuals actively. The API of the application can be used in such a way that it enables your smartphone to exchange the tracing keys periodically. This will help to locally store the unique ID of the people who have come into contact with the user (*TraceTogether* also uses this approach). If later a user is tested positive for coronavirus, this method of cryptography will also ensure the privacy and the safety of your data, as the cryptographic IDs refresh every 15 minutes and also remain anonymous.

In addition to showing the data of the number of users who have taken the self-assessment test and who have been identified as positive, a map can be shown of the nearby area where people have been identified as positive for COVID-19. Alerts through e-mail and SMS can be sent to the user while entering the red zone or containment zone. With all the above information and suggestions, other countries and regions can take a cue for working on contact-tracing apps for their respective areas and communities. This study will be helpful for various academics, researchers, data science professionals, app developers, decision-makers, policymakers, and government administrators.

REFERENCES

- [1] D. Cucinotta and M. Vanelli. 2020. WHO declares COVID-19 a pandemic. *Acta Bio Med.: Aten. Parmen* 91, 1 (2020), 157–160.
- [2] World Health Organization. 2020. Coronavirus disease 2019 (COVID-19): Situation report. Retrieved from https://www.worldometers.info/coronavirus/?utm_campaign=homeAdvegas1?%20.

- [3] The Government of India. 2020. Live updates from Worldometer. Retrieved from <https://www.worldometers.info/coronavirus/country/india/>.
- [4] H. Cho, D. Ippolito, and Y. W. Yu. 2020. Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. Retrieved from arXiv preprint arXiv:2003.11511.
- [5] M. Amit, H. Kimhi, T. Bader, J. Chen, E. Glassberg, and A. Benov. 2020. Mass-surveillance technologies to fight coronavirus spread: the case of Israel. *Nat. Med.* (26 May 2020) 1–3.
- [6] D. J. Leith and S. Farrell. 2020. Coronavirus Contact Tracing App Privacy: What Data Is Shared by The Singapore OpenTrace App? Retrieved from https://www.scss.tcd.ie/Doug.Leith/pubs/opentrace_privacy.pdf.
- [7] Aarogya Setu. 2020. MyGov. Retrieved from <https://www.mygov.in/aarogya-setu-app/>.
- [8] A. Dhindsa and S. Kaushik. 2020. The Constitutional Case against Aarogya Setu. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3610569.
- [9] Google Play. 2020. Android Playstore link. Retrieved from https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu&hl=en_IN.
- [10] IOS Store. 2020. iOS Store link. Retrieved from <https://apps.apple.com/in/app/aarogyasetu/id1505825357>.
- [11] N. Oliver, E. Letouzé, H. Sterly, S. Delataille, M. De Nadai, B. Lepri, R. Lambiotte, R. Benjamins, C. Cattuto, V. Colizza, N. de Cordes, S. P. Fraiberger, T. Koebe, S. Lehmann, J. Murillo, A. Pentland, P. N. Pham, F. Pivetta, A. A. Salah, J. Saramäki, S. V. Scarpino, M. Tizzoni, S. Verhulst, and P. Vinck. 2020. Mobile phone data and COVID-19: Missing an opportunity? Retrieved from arXiv preprint arXiv:2003.12347.
- [12] A. B. Dar, A. H. Lone, S. Zahoor, A. A. Khan, and R. Naaz. 2020. Applicability of mobile contact tracing in fighting pandemic (Covid-19): Issues, challenges, and solutions. *Cryptology ePrint Archive*, Report 2020/484.
- [13] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, and C. Fraser. 2020. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* 368 (6491).
- [14] R. Dubes and A. K. Jain. 1976. Clustering techniques: The user's dilemma. *Pattern Recog.* 8, 4 (1976), 247–260.
- [15] M. Koühne and J. Sieck. 2014. Location-based services with iBeacon technology. In *Proceedings of the 2nd International Conference on Artificial Intelligence, Modelling and Simulation*. IEEE, 315–321.
- [16] World Health Organization. 2020. Digital tools for COVID-19 contact tracing: Annex: contact tracing in the context of COVID-19, 2 June 2020. World Health Organization. Retrieved from <https://apps.who.int/iris/handle/10665/332265>.
- [17] Philipp Kindt, Trinad Chakraborty, and Samarjit Chakraborty. 2020. How Reliable is Smartphone-based Electronic Contact Tracing for COVID-19?. Retrieved from <https://arxiv.org/pdf/2005.05625.pdf>.
- [18] Aaqib Bashir Dar, Auqib Hamid Lone, Saniya Zahoor, Afshan Amin Khan, and Roohie Naaz. 2020. Applicability of Mobile Contact Tracing in Fighting Pandemic (COVID-19): Issues, Challenges and Solutions. Retrieved from https://www.researchgate.net/publication/340977670_Applicability_of_Mobile_Contact_Tracing_in_Fighting_Pandemic_COVID-19_Issues_Challenges_and_Solutions.
- [19] Jinfeng Li and Xinyi Guo. 2020. COVID-19 Contact-tracing Apps: A Survey on the Global Deployment and Challenges. Retrieved from <https://arxiv.org/ftp/arxiv/papers/2005/2005.03599.pdf>.
- [20] Assam Government FAQ. 2020. Aarogya Setu_FAQs. Retrieved from https://covid19.assam.gov.in/wp-content/uploads/2020/05/Aarogya_Setu_FAQ.pdf.
- [21] R. A. Kleinman and C. Merkel. 2020. Digital contact tracing for COVID-19. *CMAJ* 192, 24 (2020), E653–E656.
- [22] Karishma Mehrotra. 2020. Apple-Google contact tracing app: What Apple-Google Covid feature does, why it doesn't work in India. Retrieved from <https://indianexpress.com/article/explained/what-apple-google-covid-feature-does-and-why-it-doesnt-work-in-india-6480708/>.
- [23] Matteo Ciucci and Frédéric Gouardères. 2020. National COVID-19 contact tracing apps. Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies. Retrieved from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI\(2020\)652711_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf).
- [24] Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson. (7 May 2020). Retrieved from <https://www.technologyreview.com/2020/05/07/1000961/launching-mitttr-covid-tracing-tracker/>.
- [25] Dhruv Shekhar. 2020. Sensitive nature of data validates privacy concerns over Center's Aarogya Setu app; legislation with "sunset clause" can curb potential misuse. Retrieved from <https://www.firstpost.com/health/sensitive-nature-of-data-validates-privacy-concerns-over-centres-aarogya-setu-app-legislation-with-sunset-clause-can-curb-potential-misuse-8326461.html>.
- [26] Rahul Matthan. 2020. The privacy features that are built into Aarogya Setu. Retrieved from <https://www.livemint.com/opinion/columns/the-privacy-features-that-are-built-into-aarogya-setu-11586279239882.html>.
- [27] Aditi Agarwal. 2020. Changes in the privacy policy. Retrieved from <https://www.medianama.com/2020/05/223-aarogya-setu-privacy-policy-terms-of-service-update/>.

Received June 2020; revised July 2020; accepted July 2020